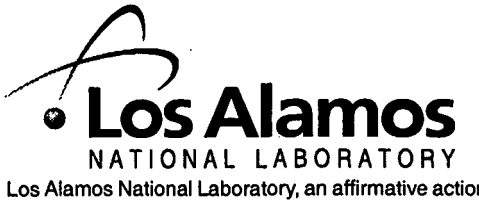
LA-UR- 02-7592

Approved for public release;
distribution is unlimited.

Title: A RISK-BASED APPROACH TO DESIGNING EFFECTIVE SECURITY FORCE TRAINING EXERCISES

Author(s): Terry F. Bott
Stephen W. Eisenhawer

Submitted to: INMM 44th Annual Meeting
July 13-17-2003
Phoenix, AZ



Form 836 (8/00)

A Risk-Based Approach to Designing Effective Security Force Training Exercises

T. F. Bott and S. W. Eisenhawer
Probabilistic Risk Analysis, Group D-11
Los Alamos National Laboratory

The effectiveness of a security force in protecting a nuclear facility is often evaluated using training exercises that pit a group of simulated attackers against a security team. In the situation studied here, a security force was regularly tested by a regulatory body with the responsibility for security oversight. It was observed that the regulators were continually imposing more challenging security scenarios by assigning increasingly sophisticated facility knowledge to the attackers. Not surprisingly, the security forces' assessed effectiveness decreased until eventually they were unable to successfully resist the attacks. Security managers maintained that the knowledge attributed to the attackers was becoming increasingly unrealistic and feared they would be forced to concentrate resources on unrealistic scenarios at the expense of more credible threats.

The validity of the security forces' complaints was investigated by performing a risk analysis using the Logic Evolved Decision (LED) method. An exhaustive list of possible attack scenarios was developed using a deductive logic model called a process tree. The likelihood of success from the attacker's viewpoint was estimated for each of the scenarios using an approximate reasoning inference model that utilizes qualitative input data and expresses uncertainty using fuzzy measures. This approach provided a metric for determining which scenarios offered the best overall likelihood of success for the adversary, and hence which attacks were most risky from the defender's standpoint.

The results of the analysis demonstrated that the attack scenarios with the highest likelihood of success given an actual attempt also carried the highest risk to the adversary of prevention or interdiction before an attempt was even made. The interdiction and prevention likelihood are high principally because of the actions required to collect highly detailed target and facility information. Such information is controlled and accessible by a restricted set of personnel. Locating and recruiting an individual with the requisite information represents a risk to the attacker that is normally ignored. There was a strong tradeoff between the adversary's risk of interdiction arising from the attempt to collect more information before the attack versus settling for less information and mounting an attack with a lower likelihood of success. This strongly suggests that more realistic gaming best serves the objective of improved security.